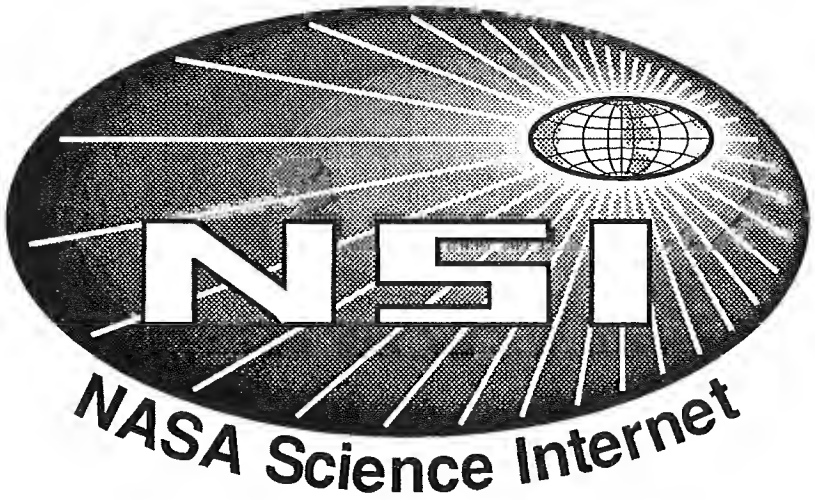

NSIUWG
SECURITY SUB-GROUP

SECURITY SUB-GROUP

Security - How and Why

GAO audit and report critical of NASA network management

NASA image is Vulnerable - Any breach becomes a "NASA Problem"

Security of the network requires adequate end-node security

NSI cannot require compliance, but all policies and procedures will be consistent with NASA policy. No "extraordinary" measures will be required - however, common sense will.

NSI will provide the user community with assistance and tools to allow non-interference management of tail sites.

NSI SECURITY

TOOLKITS

- Enable remote sites to self-evaluate their vulnerabilities
- Working w/NIST to model threats and identify existing tools
- Evaluating LLNL "SPI" and CMU "COPS" packages
- Priority being given to developing a set of UNIX tools
- Will update and revise the VMS (SPAN) toolkit
- Goal is VMS/UNIX equivalent tools
- NSI-Approved and NSI-Developed

SECURITY SUB-GROUP

SECURITY POLICIES AND DOCUMENTATION

Goal: To establish a network-wide "Security Baseline"

All policy will be NHB 2410.9-compliant

Will address UNIX & VMS, DECnet & TCP/IP (OSI as appropriate)

Will reflect required Risk Analysis elements

Will include Audit Trail guidance based on inputs from FBI and Justice Depts

Currently in draft form - Expected to publish in FY90

SECURITY SUB-GROUP

RISK ANALYSIS & MANAGEMENT

Government sites required to perform their own. NSI will provide guidance.

NSI will do a "Network" Risk Analysis.

NSI is working with Code NTD to develop a uniform NASA approach consistent with AIS guidelines.